PATENT
81784.0289
Express Mail Label No. EV 324 110 896 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Yutaka KANEKO	Examiner: Not assigned
Serial No: Not assigned	
Filed: November 3, 2003	
For: Optical Disk Drive, Optical Disk, Security Control Method for Optical Disk Drive, and Security Control Program for Optical Disk Drive	

TRANSMITTAL OF PRIORITY DOCUMENT

Mail Stop PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2002-360851 which was filed December 12, 2002, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: November 3, 2003

By: _____
Anthony J. Orler
Registration No. 41,232
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

Translation of Priority Certificate

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application:	**December 12, 2002**
Application Number:	**Patent Application No. 2002-360851**
[ST.10/C]:	**[JP2002-360851]**
Applicant(s):	**SANYO ELECTRIC CO., LTD.**

July 2, 2003

Commissioner, Japan Patent Office
Shinichiro Ota

Priority Certificate No. 2003-3052420

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１２月１２日

出願番号
Application Number:　特願２００２－３６０８５１

[ST.10/C]:　[ＪＰ２００２－３６０８５１]

出願人
Applicant(s):　三洋電機株式会社

２００３年　７月　２日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０５２４２０

【書類名】　特許願
【整理番号】　JAB1020113
【提出日】　平成14年12月12日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　7/00
　　G06F 11/00
【発明者】
　【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
　【氏名】　金子　豊
【特許出願人】
　【識別番号】　000001889
　【氏名又は名称】　三洋電機株式会社
【代理人】
　【識別番号】　100075258
　【弁理士】
　【氏名又は名称】　吉田　研二
　【電話番号】　0422-21-2340
【選任した代理人】
　【識別番号】　100096976
　【弁理士】
　【氏名又は名称】　石田　純
　【電話番号】　0422-21-2340
【手数料の表示】
　【予納台帳番号】　001753
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　光ディスク装置、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラム

【特許請求の範囲】

【請求項１】　データとデータに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段と、

光ディスクからデータ及びセキュリティ情報を読み出す読取手段と、

データを読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段と、

を備えることを特徴とする光ディスク装置。

【請求項２】　データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクからデータを読み出す光ディスク装置であって、

前記光ディスクからデータ及びセキュリティ情報を読み出す読取手段と、

データに読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段と、

を備えることを特徴とする光ディスク装置。

【請求項３】　請求項１又は２に記載の光ディスク装置において、

前記セキュリティ情報は、連続するビット列で表される情報であり、

前記アクセス制御手段は、前記複数箇所からセキュリティ情報として読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列の正しいビット値とすることを特徴とする光ディスク装置。

【請求項４】　請求項１～３のいずれか１つに記載の光ディスク装置におい

て、

前記読取手段によって読み出されたデータの誤り頻度を検出するエラー検出手段を更に含み、

前記アクセス制限手段は、前記エラー検出手段によって得られたデータの誤り頻度に基づいてセキュリティ情報を補正することを特徴とする光ディスク装置。

【請求項５】　記録対象となるデータと、当該データに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段を備えることを特徴とする光ディスク装置。

【請求項６】　記録対象となるデータと、当該データに対するセキュリティ情報とが記録された光ディスクであって、同一のセキュリティ情報が複数箇所に記録されていることを特徴とする光ディスク。

【請求項７】　データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理方法であって、

管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、

前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程と、

を含み、

前記正当セキュリティ情報を前記管理対象となるデータの処理に供することを特徴とする光ディクス装置のセキュリティ管理方法。

【請求項８】　請求項７に記載の光ディスク装置のセキュリティ管理方法において、

前記セキュリティ情報は、連続するビット列で表される情報であり、

前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることを特徴とする光ディスク装置のセキュリティ管理方法。

【請求項９】　請求項７又は８に記載の光ディスク装置のセキュリティ管理

方法において、

前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに含み、

前記セキュリティ情報決定工程は、前記誤り頻度に基づいて正しいセキュリティ情報を決定することを特徴とする光ディスク装置のセキュリティ管理方法。

【請求項１０】　データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理プログラムであって、

コンピュータに、

管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、

前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程と、

を含む処理を実行させることを特徴とする光ディクス装置のセキュリティ管理プログラム。

【請求項１１】　請求項１０に記載の光ディスク装置のセキュリティ管理プログラムにおいて、

前記セキュリティ情報は、連続するビット列で表される情報であり、

前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることを特徴とする光ディスク装置のセキュリティ管理プログラム。

【請求項１２】　請求項１１又は１２に記載の光ディスク装置のセキュリティ管理プログラムにおいて、

コンピュータに、前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに実行させ、

前記セキュリティ情報決定工程において、前記誤り頻度に基づいて正しいセキュリティ情報を決定することを特徴とする光ディスク装置のセキュリティ管理プ

ログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンパクトディスク及びデジタル多目的ディスク等の光ディスクシステムにおいてセキュリティ性及びアクセス性を向上した光ディスク装置、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラム方法に関する。

【０００２】

【従来の技術】

動画記録等の大容量データ記録の必要性が高まり、高密度記録型コンパクトディスク（ＨＤ－Ｂｕｒｎ－ＣＤ：Ｈｉｇｈ－Ｄｅｎｓｉｔｙ－Ｂｕｒｎ　ｔｙｐｅ）及びデジタル多目的ディスク（ＤＶＤ）が広く使用されている。

【０００３】

このような大容量の記憶装置においては、そこに記憶されたデータの改竄や、アクセス権を持たない者からの不正なデータの読み出しを防ぐことがセキュリティ上の課題となっている。

【０００４】

特開平２００１－３５０９２号公報には、光ディスク等のリムーバブルメモリのセキュリティを向上する技術が開示されている。当該技術では、リムーバブルメモリのメモリ空間において一般ユーザが書き換え不能な管理領域を予め定めておき、その管理領域にユーザのパスワード等のセキュリティ情報を埋め込み、リムーバブルメモリにアクセスする際にはユーザから確認用の情報の入力を行わせ、管理領域に埋め込まれたセキュリティ情報とユーザが入力した確認用の情報とを対比して所定の条件を満たせばリムーバブルメモリへのアクセスを可能にする。

【０００５】

【特許文献１】

特開平２００１－３５０９２号公報

【０００６】

【発明が解決しようとする課題】

しかしながら、上記従来技術では、リムーバブルディスク上に一般ユーザが容易にアクセスできない管理領域を設けておく必要があった。管理領域にはリムーバブルディスク上に記録される全データに対する管理データが記録されるため、管理領域として予め広い記憶領域を割り当てておく必要があり、実際に利用できる記録領域が減少する等の問題があった。

【０００７】

また、上記従来技術では、リムーバブルディスク上の全データに対するセキュリティ情報が管理領域に集中して記録される。そのため、セキュリティ情報を盗み見ようとする者がセキュリティ情報を発見し易くなり、セキュリティ情報の漏洩や改竄等の問題が起こりやすい状況にあった。

【０００８】

さらに、データを記録又は読取する際に、ディスク装置のヘッドをリムーバブルディスク上のデータ記録領域と管理領域との間で頻繁に移動させる必要がある。そのため、データへのアクセス時間が長くなる問題があった。

【０００９】

本発明は、上記従来技術の問題を鑑み、少なくとも上記課題の一つを解決するべく、改良されたセキュリティ管理を可能とする光ディスク装置、光ディスク、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラムを提供することを目的とする。

【００１０】

【課題を解決するための手段】

上記課題を解決できる本発明は、データとデータに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段と、光ディスクからデータ及びセキュリティ情報を読み出す読取手段と、データを読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の

高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段とを備えることを特徴とする光ディスク装置である。

【００１１】

ここで、本発明は、データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクからデータを読み出す光ディスク装置であって、前記光ディスクからデータ及びセキュリティ情報を読み出す読取手段と、データに読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段とを備えることを特徴とする。

【００１２】

より具体的には、前記セキュリティ情報は、連続するビット列で表される情報であり、前記アクセス制御手段は、前記複数箇所からセキュリティ情報として読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列の正しいビット値とすることを特徴とすることが好適である。

【００１３】

さらに、上記光ディスク装置において、前記読取手段によって読み出されたデータの誤り頻度を検出するエラー検出手段を更に含み、前記アクセス制限手段は、前記エラー検出手段によって得られたデータの誤り頻度に基づいてセキュリティ情報を補正することが好ましい。

【００１４】

上記課題を解決できる本発明の別の態様は、記録対象となるデータと、当該データに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段を備えることを特徴とする光ディスク装置である。

【００１５】

上記課題を解決できる本発明の別の態様は、記録対象となるデータと、当該デ

ータに対するセキュリティ情報とが記録された光ディスクであって、同一のセキュリティ情報が複数箇所に記録されていることを特徴とする光ディスクである。

【００１６】

上記課題を解決できる本発明の別の態様は、データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理方法であって、管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程とを含み、前記正当セキュリティ情報を前記管理対象となるデータの処理に供することを特徴とする。

【００１７】

より具体的には、前記セキュリティ情報は、連続するビット列で表される情報であり、前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることが好適である。

【００１８】

さらに、上記光ディスク装置のセキュリティ管理方法において、前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに含み、前記セキュリティ情報決定工程は、前記誤り頻度に基づいて正しいセキュリティ情報を決定することが好ましい。

【００１９】

上記課題を解決できる本発明は、データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理プログラムであって、コンピュータに、管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程とを含む処理を実行させることを特徴とする

。

【００２０】

より具体的には、前記セキュリティ情報は、連続するビット列で表される情報であり、前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることが好適である。

【００２１】

さらに、上記光ディスク装置のセキュリティ管理プログラムにおいて、コンピュータに、前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに実行させ、前記セキュリティ情報決定工程において、前記誤り頻度に基づいて正しいセキュリティ情報を決定することが好ましい。

【００２２】

【発明の実施の形態】

本発明の実施の形態について、図を参照して詳細に説明する。

【００２３】

＜装置構成＞

本発明の実施の形態における光ディスク装置１００の構成は、図１のように、制御部１０、記憶部１２、データエンコーダ１４、光学系制御部１６、光学ヘッド１８、ＡＴＩＰデコーダ２０、データデコーダ２２、モータ制御部２４、モータ２６及びインターフェース２８から基本的に構成される。

【００２４】

光ディスク装置１００は、インターフェース２８を介して外部装置と情報伝達可能に接続され、例えば外部に置かれたホストコンピュータ等に対してデータの入出力を行うことができる。

【００２５】

制御部１０は、記憶部１２、データエンコーダ１４、光学系制御部１６、データデコーダ２２及びインターフェース２８と情報伝達可能に接続され、記憶部１２に格納された制御プログラムを実行することによって光ディスク装置１００の制御を統括する。制御部１０は、インターフェース２８から受け取ったデータを

記憶部１２に一旦格納し、随時読み出してデータエンコーダ１４に送出する。

【００２６】

データエンコーダ１４は、制御部１０からの制御命令に従って、受信したデータを光ディスクに記録するためのデータフォーマットに変換し、光学系制御部１６に出力する。

【００２７】

光学系制御部１６は、制御部１０からのデータ書込み命令を受け、光学ヘッド１８を制御することによってデータエンコーダ１４から受けたデータを光ディスクに書き込む。また、制御部１０からのデータ読み込み命令を受け、光学ヘッド１８を制御することによって光ディスクから読み出したデータをデータデコーダ２２及びＡＴＩＰデコーダ２０に出力する。

【００２８】

光学ヘッド１８は、レーザ、レンズ、駆動装置等を含み、光ディスク上にデータを書込み、又は光ディスクからデータを読み取る。例えば、ＤＶＤでは６５０ｎｍの波長のレーザを用いることができる。

【００２９】

ＡＴＩＰデコーダ２０は、光ディスクから抽出されるウォブル信号からＡＴＩＰ（Ａｂｓｏｌｕｔｅ　Ｔｉｍｅ　Ｉｎ　Ｐｒｅ－ｇｒｏｏｖｅ）アドレスを復調し、モータ制御部２４に出力する。

【００３０】

データデコーダ２２は、光ディスクから読み出されたデータを受けて、受信したデータの復調を行い、制御部１０へ送出する。

【００３１】

モータ制御部２４は、ＡＴＩＰデコーダ２０からＡＴＩＰアドレスを受けて、スピンドルモータ２６を制御することによって光ディスクの回転を調整する。例えば、ＡＴＩＰアドレスと同期をとって光ディスクを線速度一定に回転制御する。

【００３２】

＜データ及びセキュリティ情報の記録処理＞

以下、図を参照して、本実施の形態におけるデータ及びセキュリティ情報の記録処理について詳細に説明する。本実施の形態における記録処理は、図２のフローチャートに示す各工程をプログラム化して記憶部１２に記憶させておき、制御部１０で実行することによって行うことができる。

【００３３】

ステップＳ１０では、記録対象となるデータを外部装置から受信し、受信したデータをデータブロックに分割する。データブロックとしては、例えば、リード・ソロモン積符号方式におけるＥＣＣ（積符号）データブロックを用いることができる。このリード・ソロモン積符号方式では、３２ｋＢの実データに対して５ｋＢの誤り訂正用の冗長データ（パリティ）が付加された合計３７ｋＢのＥＣＣ（積符号）データブロックによって誤り訂正が行われる。

【００３４】

図３に示すように、データを１バイト単位のデータＤ０，Ｄ１・・・Ｄｎ毎に、所定のデータ単位ｋ毎に縦方向に折り返しながら読み出した順に横方向に行列配置する。さらに、図４に示すように、データ$D_{i,j}$（ｉ，ｊは行列番号）がブロック化されると、各々の行及び列毎に冗長データＰＩ，ＰＯを付与する。横方向の各行を内符号と呼び、縦方向の各列を外符号と呼ぶ。通常、内符号系列ＲはＲＳ（１８２，１７２，１１）、外符号系列ＣはＲＳ（２０８，１９２，１７）と記載される。ここで、ＲＳ（ｎ，ｋ，ｄ）において、ｎは符号長、ｋは情報記号長、ｄは符号語間の最小距離を示す。

【００３５】

このリード・ソロモン積符号方式は強力な誤り訂正機能を有しており、ＥＣＣデータブロック内に生ずる僅かな誤りを完全に修正することができる。本発明では、この強力な誤り訂正機能を利用する。

【００３６】

ステップＳ１２では、外部装置からセキュリティ情報を受信し、受信したセキュリティ情報を複数のＥＣＣデータブロックに埋め込む。セキュリティ情報を埋め込むＥＣＣデータブロックの数は記録処理前に予め定めておくことができる。

【００３７】

例えば、記録対象となるデータに対するセキュリティ情報が３バイトの情報量であり、その値が５５ｈ，７６ｈ，９８ｈであったとする。１つのセキュリティ情報を５つのＥＣＣデータブロックに埋め込むことと予め設定されている場合、図５に示すように、記録対象となるデータから得られた５つのＥＣＣデータブロックにおいて最初のデータ値から順にセキュリティ情報に置き換える。

【００３８】

このとき、セキュリティ情報を埋め込むＥＣＣデータブロックはランダムに選択しても良い。また、セキュリティ情報を埋め込む位置は予め定められていれば、ＥＣＣデータブロックにおけるデータ領域のいずれの場所に埋め込んでも良い。

【００３９】

さらに、セキュリティ情報が複数ある場合には、それらのセキュリティ情報を１つのＥＣＣデータブロックに埋め込んでも良い。ただし、１つのＥＣＣデータブロックに埋め込むセキュリティ情報数は、記録及び読取を通じて発生する誤りをリード・ソロモン積符号方式で訂正できる程度に抑えることが好ましい。従って、セキュリティ情報の情報量が誤り訂正できない程度に大きい場合には、セキュリティ情報を分割してＥＣＣデータブロックに振り分けて埋め込むことが好適である。

【００４０】

例えば、内符号系列ＲＳ（１８２，１７２，１１）及び外符号系列ＲＳ（２０８，１９２，１７）のリード・ソロモン積符号方式を用いた場合、バースト誤りが生じないものとすると、誤り訂正可能なデータの個数は９３バイトとなる。

【００４１】

ステップＳ１４では、セキュリティ情報が埋め込まれたＥＣＣデータブロックの情報を実際に光ディスクに記録する。例えば、セキュリティ情報が埋め込まれたことをディスクの管理情報に記録しておくことが好適である。

【００４２】

以上の処理によって、光ディスク上にデータ及びセキュリティ情報に記録することができる。

【００４３】

＜データ及びセキュリティ情報の読取処理＞

以下、図を参照して、本実施の形態におけるデータ及びセキュリティ情報の読取処理について詳細に説明する。本実施の形態における記録処理は、図６のフローチャートに示す各工程をプログラム化して記憶部１２に記憶させておき、制御部１０で実行することによって行うことができる。

【００４４】

ステップＳ２０では、外部装置からの指令を受けて、光ディスク装置の管理情報等を読み出し、読み出し対象となるデータにセキュリティ情報が記録されているか否かを確認する。セキュリティ情報が埋め込まれていればステップＳ２２に処理を移行し、セキュリティ情報が埋め込まれていなければステップＳ３０に処理を移行する。

【００４５】

ステップＳ２２では、読み出し対象となるデータに埋め込まれているセキュリティ情報を抽出して外部装置に送出する。

【００４６】

まず、光ディスク上のデータ領域にアクセスし、読み出し対象となるデータをＥＣＣデータブロックに再構築する。次に、リード・ソロモン積符号方式に基づいて、ＥＣＣデータブロックのデータの誤り訂正を行う。このとき、ＥＣＣデータブロック間においてデータの誤り率の比較を行い、誤り率が高いＥＣＣデータブロックにセキュリティ情報が埋め込まれているものと判断し、セキュリティ情報が埋め込まれていると判断されたＥＣＣデータブロックの所定位置からセキュリティ情報を抽出する。

【００４７】

例えば、図５の例のようにＥＣＣデータブロックの最初の３バイトにセキュリティ情報が埋め込まれたデータを読み出し、図７に示すようにＥＣＣデータブロックが再現されたものとする。ここで、黒塗りのデータはデータの記録処理又はデータの読取処理の際に誤りが生じたデータを示す。

【００４８】

各ＥＣＣデータブロックには、一般的にほぼ同じ確率でデータの誤りが生ずる。セキュリティ情報自体がデータの誤りであるものと認識されるため、セキュリティ情報が埋め込まれたＥＣＣデータブロックのデータの誤り率は、セキュリティ情報が埋め込まれていないＥＣＣデータブロックの誤り率よりも高くなる。図７の例では、ＥＣＣデータブロック１～５にセキュリティ情報が埋め込まれているため、他のＥＣＣデータブロックよりも誤り率が高くなっており、これらのＥＣＣデータブロックからセキュリティ情報を抽出すれば良いことが判断できる。

【００４９】

このとき、なんらかの偶発的事情により、ＥＣＣデータブロック８のように誤り率が高くなった場合、本来セキュリティ情報が埋め込まれていないＥＣＣデータブロックからもセキュリティ情報が抽出されることとなる。この場合の処理については後に詳細に説明する。

【００５０】

ステップＳ２４では、複数のＥＣＣデータブロックから抽出されたセキュリティ情報を比較し、セキュリティ情報の誤りを修正する。

【００５１】

例えば、図７の例から読み出されたセキュリティ情報の最上位のデータが、５５ｈ，７５ｈ，５５ｈ，４Ｄｈ及び５５ｈとして抽出されたものとする。また、セキュリティ情報が埋め込まれていなかったＥＣＣデータブロックからも９７ｈという情報が誤って抽出されたものとする。

【００５２】

そこで、図８に示すように、抽出されたセキュリティ情報を同一ビット列毎に比較し、高い頻度で現れるビット値をそのビット列における正しいビット値として採用する。例えば、最上位ビットは０，０，０，０，０，１であり、「０」が５つ及び「１」が１つ出現するので、最上位ビットの正しいビット値は「０」とする。

【００５３】

また、セキュリティ情報の抽出元となったＥＣＣデータブロックのデータ誤り率によって各ビット列に重み付けをして処理を行うことも好適である。すなわち

、抽出元となったＥＣＣデータブロックのデータ誤り率が高い場合には、そこから抽出されたセキュリティ情報が誤っている可能性も高くなると考えられるため、データ誤り率の高いＥＣＣデータブロックから抽出されたセキュリティ情報の重要性が低く見積もられるように重み付けする。

【００５４】

このように、複数抽出されたセキュリティ情報を比較し、最も出現頻度が高いセキュリティ情報を正当なセキュリティ情報として採用することによって、データに埋め込んだセキュリティ情報に誤りが発生したり、セキュリティ情報が埋め込まれていないＥＣＣデータブロックから誤ってセキュリティ情報が抽出されたりした場合にも、正しいセキュリティ情報を得られる可能性を高めることができる。

【００５５】

ステップＳ２６では、データの読み出しを制限するか否かを判断するために、ユーザ等から確認情報を取得する。この確認情報は、外部装置から取得される。

【００５６】

ステップＳ２８では、ステップＳ２４で抽出された正当なセキュリティ情報と、ステップＳ２６で取得された確認情報が比較される。抽出された正当なセキュリティ情報と確認情報が一致していればステップＳ３０に処理を移行し、一致していなければステップＳ３２に処理を移行する。

【００５７】

このとき、セキュリティ情報に誤りが多く発生していたり、バースト誤り等の影響によりセキュリティ情報が多く誤って読み出されたりした場合に、ステップＳ２４においてセキュリティ情報を完全に修正できなくなることも考慮して、抽出された正当なセキュリティ情報と確認情報とが完全に一致していなくとも、ある程度一致していれば良いものとすることもできる。

【００５８】

ステップＳ３０では、アクセスが許可できるものとして、読み出し対象となるデータを光ディスクから読み出して外部装置に送信する。外部装置は、ユーザにデータを提示する。一方、ステップＳ３２では、データの読み出しを拒否する。

例えば、光ディスクを強制的に装置から排出させる処理等を行っても良い。

【００５９】

なお、本実施の形態では、リード・ソロモン積符号化方式に基づいてデータの誤り訂正を行うものとして説明を行ったが、これに限られるものではなく、他の誤り訂正方式を用いた場合でも同様に処理することができる。

【００６０】

以上のように、本実施の形態によれば、光ディスクに記録されたデータにユーザ名、パスワード、暗号鍵等のセキュリティ情報を埋め込むことによって、セキュリティ性を高めたデータの保存が可能となる。

【００６１】

その結果、例えば、セキュリティ情報がデータに埋め込まれて記録されるため、光ディスク上に設ける管理領域が小さくすることができる。さらに、光ディスク上でセキュリティ情報が分散して記録されるため、セキュリティ情報の漏洩や改竄を行い難くなり、アクセス時間を短縮できる。

【００６２】

【発明の効果】

本発明によれば、コンパクトディスク及びデジタル多目的ディスク等の光ディスクシステムにおいてセキュリティ性及びアクセス性を向上した光ディスク装置、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラム方法を実現することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態における光ディスク装置の構成を示すブロック図である。

【図２】　本発明の実施の形態におけるデータ記録処理のフローチャートを示す図である。

【図３】　データ列からのデータブロックの構成を説明する図である。

【図４】　リード・ソロモン積符号方式の積符号データブロックの例を示す図である。

【図５】　本実施の形態におけるデータブロックへのセキュリティ情報の埋

め込み処理を説明する図である。

【図６】　本発明の実施の形態におけるデータ読取処理のフローチャートを示す図である。

【図７】　本発明の実施の形態におけるデータブロックからのセキュリティ情報の読み出し処理を説明する図である。

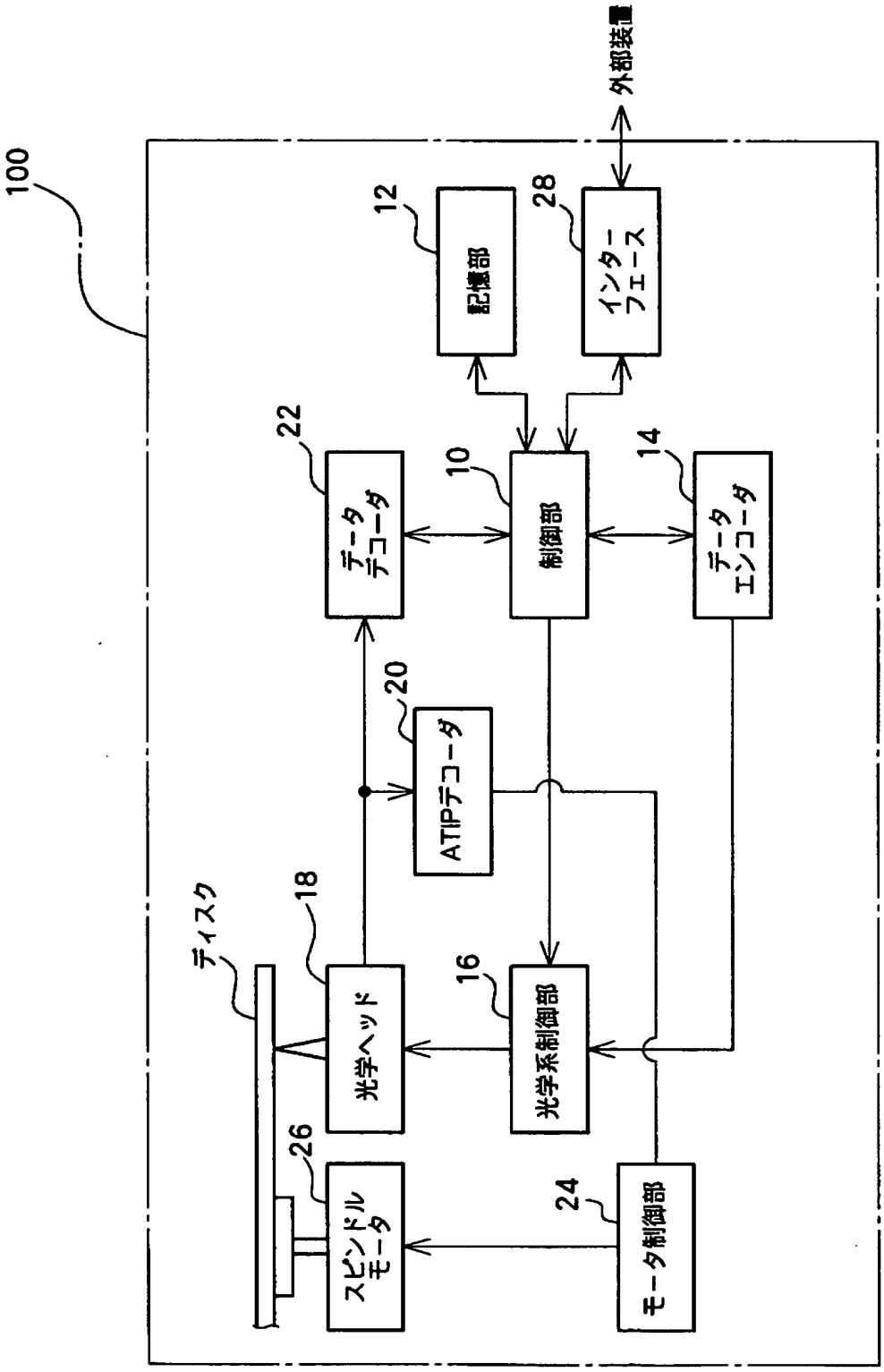
【図８】　本発明の実施の形態におけるセキュリティ情報の比較・修正処理を説明する図である。

【符号の説明】

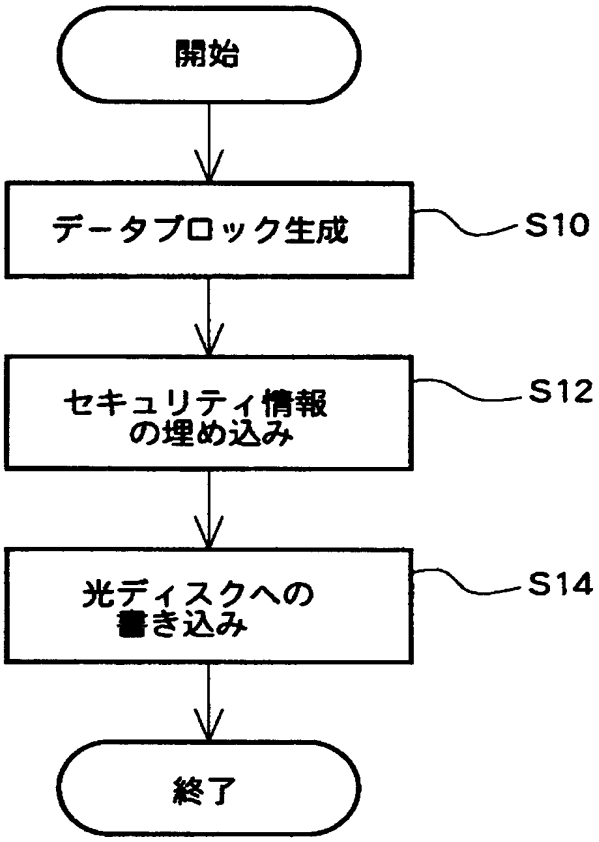
１０　制御部、１２　記憶部、１４　データエンコーダ、１６　光学系制御部、１８　光学ヘッド、２０　デコーダ、２２　データデコーダ、２４　モータ制御部、２６　スピンドルモータ、２８　インターフェース、１００　光ディスク装置。

【書類名】　　図面

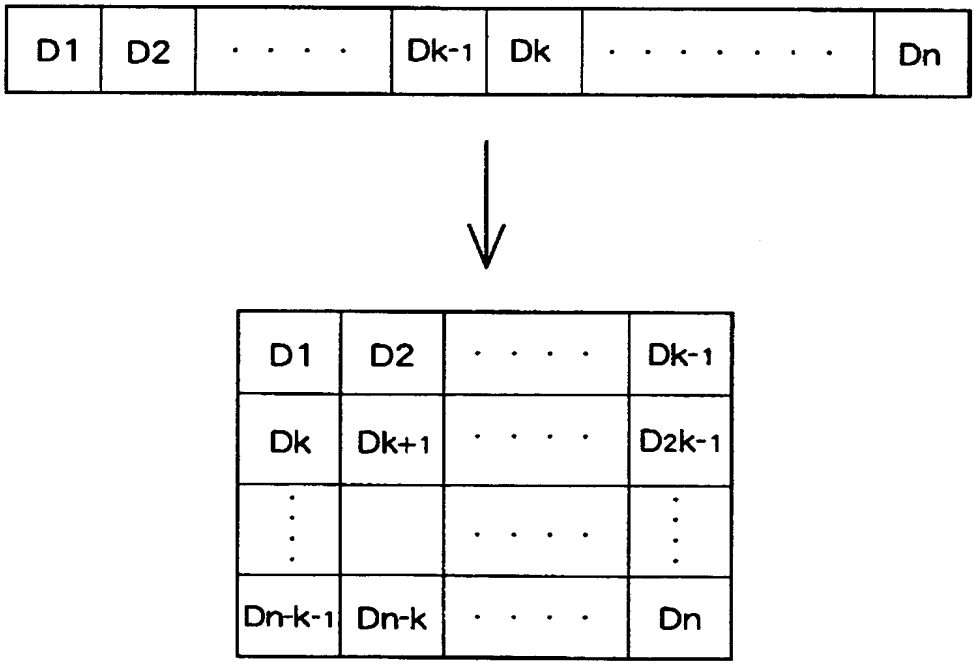
【図１】


100
外部装置
12
記憶部
28
インターフェース
22
データデコーダ
10
制御部
14
データエンコーダ
20
ATIPデコーダ
ディスク
18
光学ヘッド
16
光学系制御部
26
スピンドルモータ
24
モータ制御部

【図２】

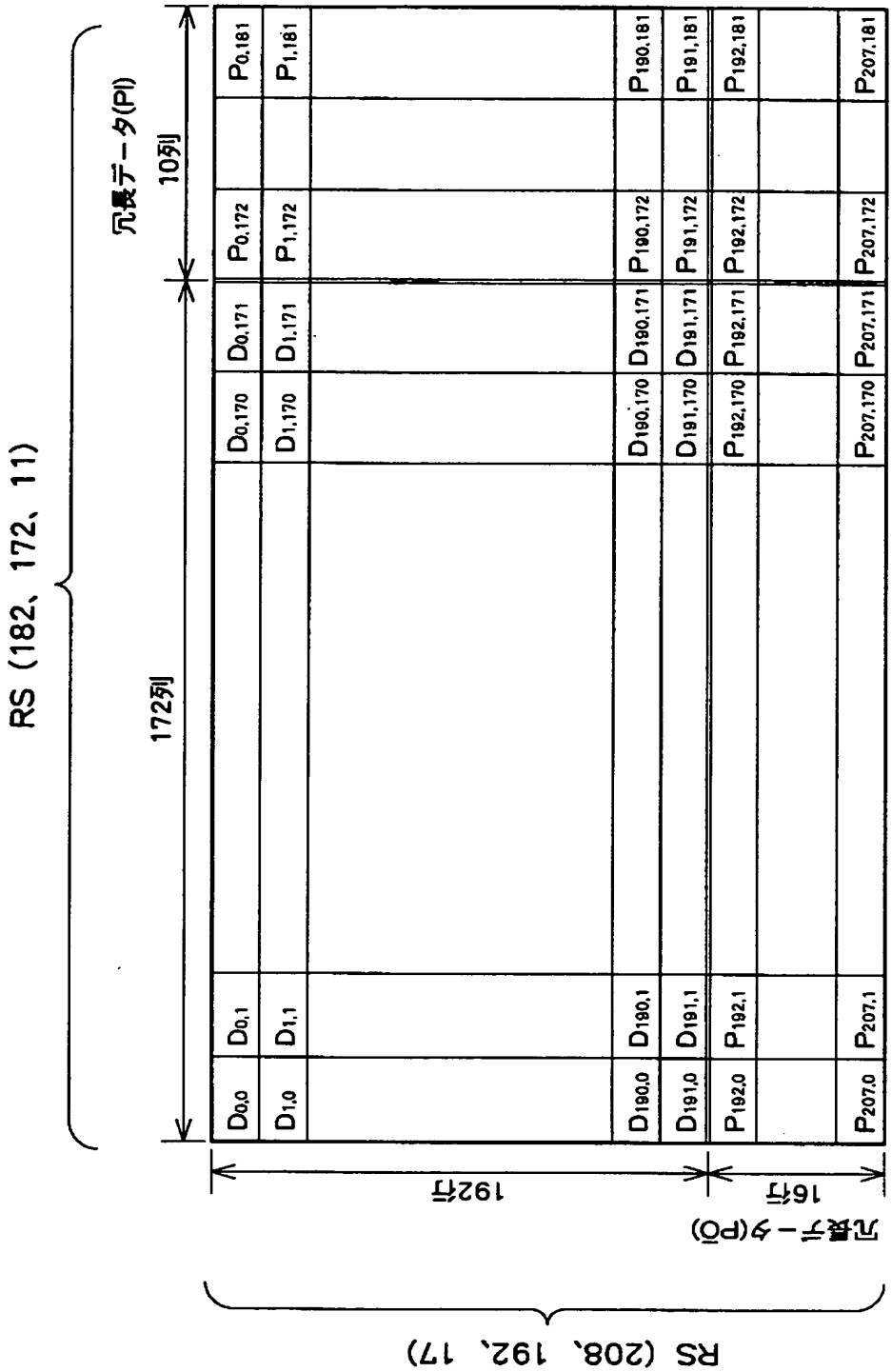


【図３】

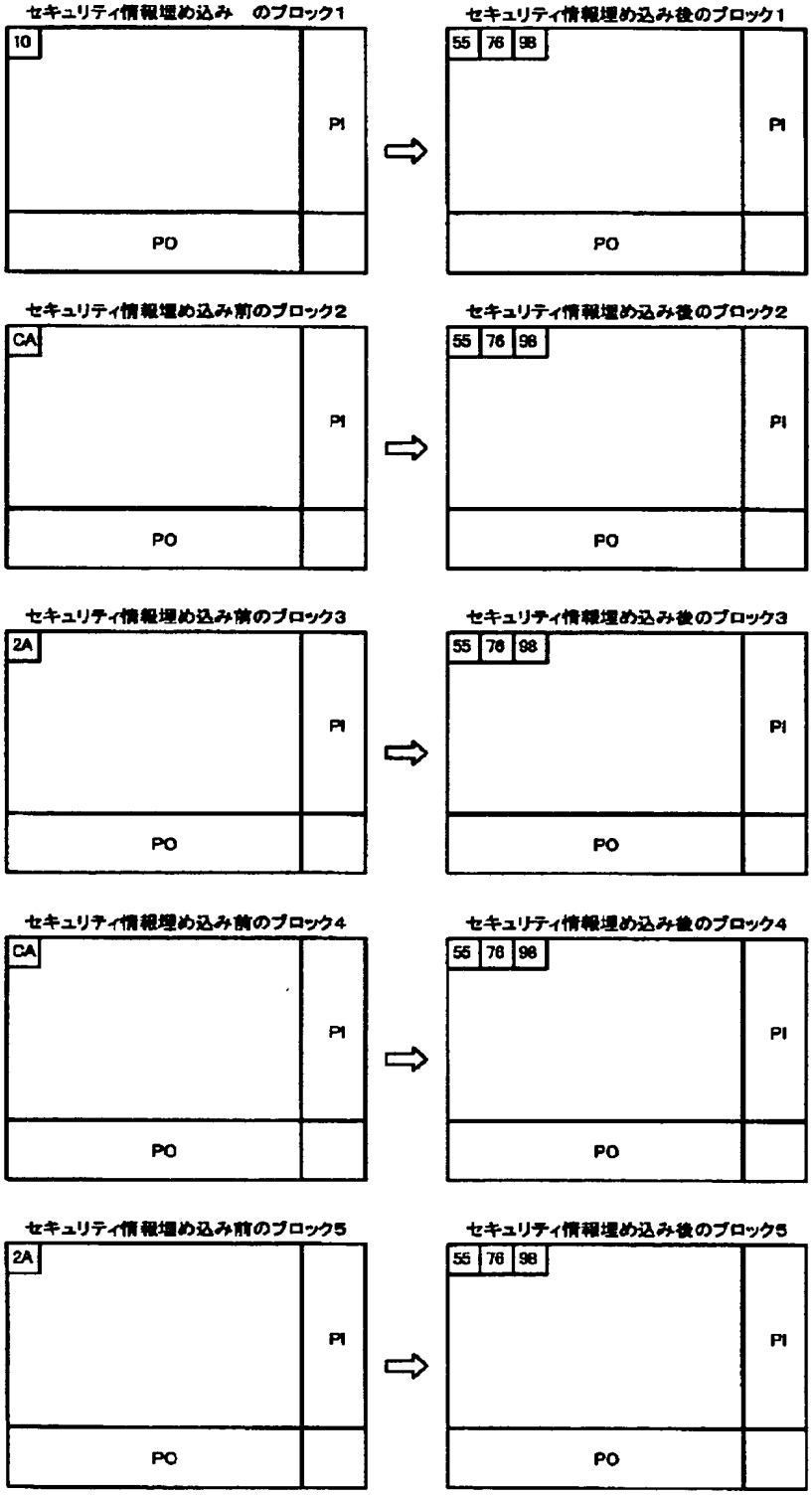


出証特２００３－３０５２４２０

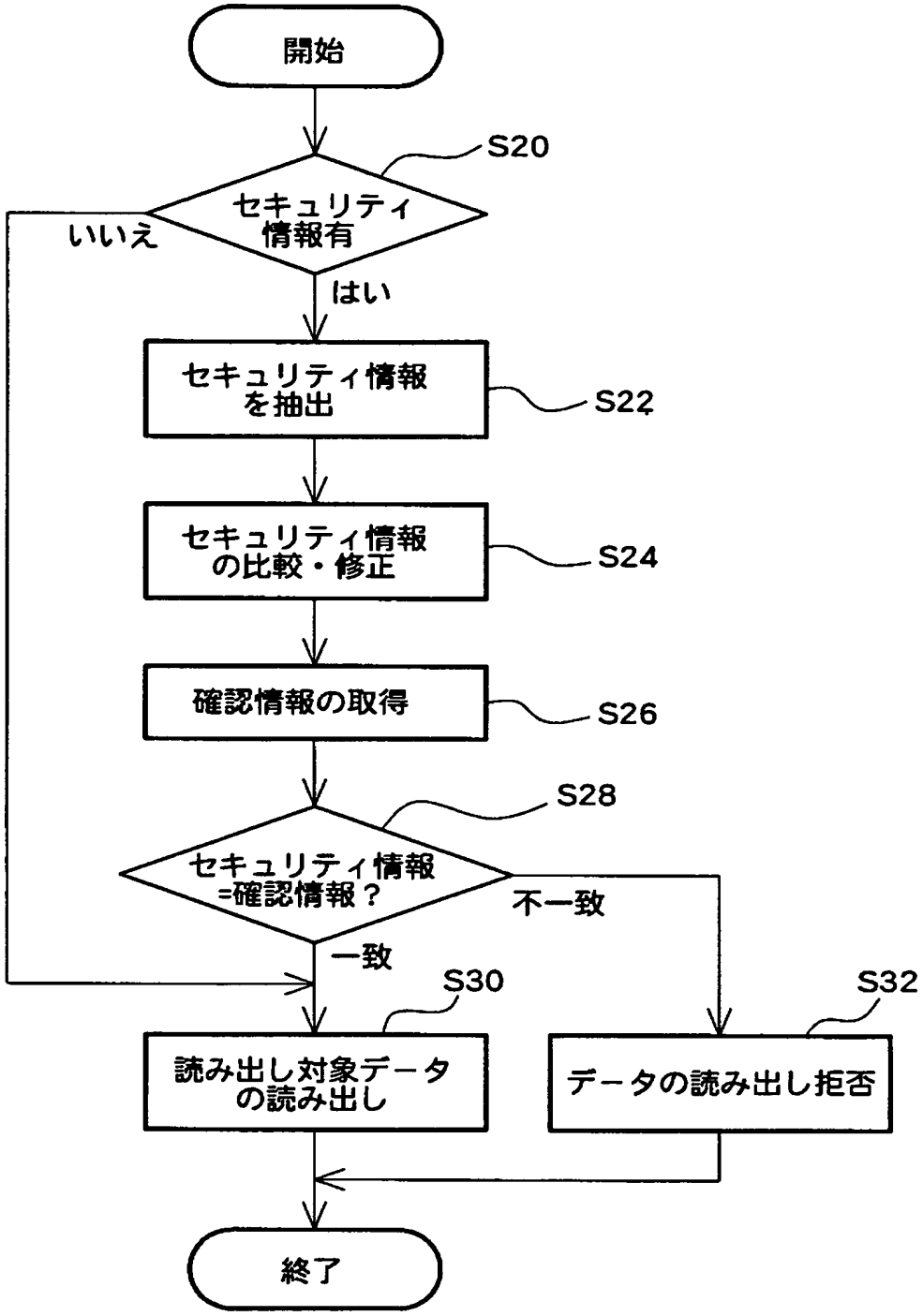
【図４】



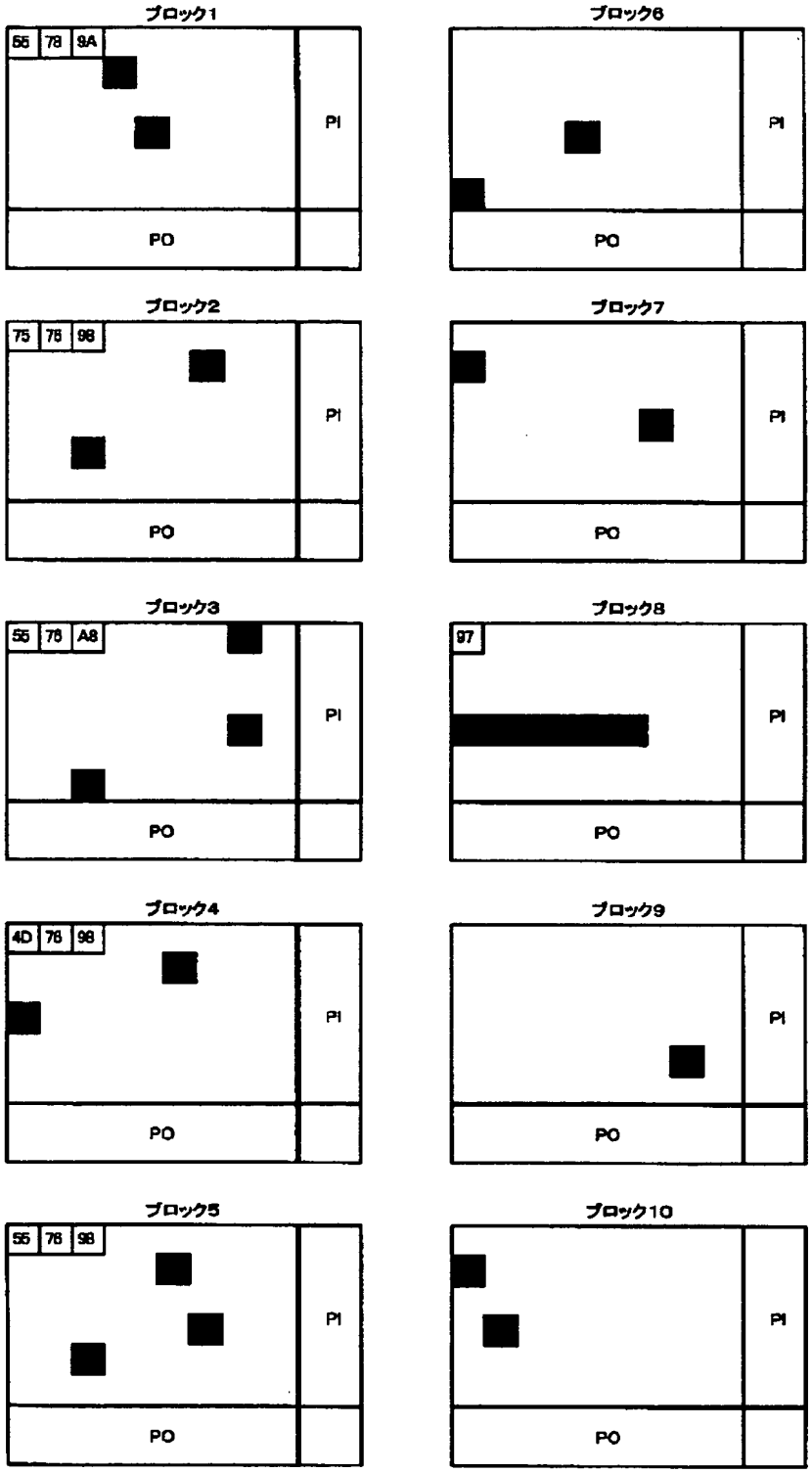
【図５】


セキュリティ情報埋め込み　のブロック1
10
PI
PO
セキュリティ情報埋め込み後のブロック1
55 76 98
PI
PO
セキュリティ情報埋め込み前のブロック2
CA
PI
PO
セキュリティ情報埋め込み後のブロック2
55 76 98
PI
PO
セキュリティ情報埋め込み前のブロック3
2A
PI
PO
セキュリティ情報埋め込み後のブロック3
55 76 98
PI
PO
セキュリティ情報埋め込み前のブロック4
CA
PI
PO
セキュリティ情報埋め込み後のブロック4
55 76 98
PI
PO
セキュリティ情報埋め込み前のブロック5
2A
PI
PO
セキュリティ情報埋め込み後のブロック5
55 76 98
PI
PO

【図６】


開始
S20
セキュリティ情報有
いいえ
はい
セキュリティ情報を抽出
S22
セキュリティ情報の比較・修正
S24
確認情報の取得
S26
S28
セキュリティ情報=確認情報？
不一致
一致
S30
S32
読み出し対象データの読み出し
データの読み出し拒否
終了

【図７】


ブロック1
55
78
9A
PI
PO
ブロック6
PI
PO
ブロック2
75
78
98
PI
PO
ブロック7
PI
PO
ブロック3
55
78
A8
PI
PO
ブロック8
97
PI
PO
ブロック4
4D
78
98
PI
PO
ブロック9
PI
PO
ブロック5
55
78
98
PI
PO
ブロック10
PI
PO

【図８】

	セキュリティ情報	セキュリティ情報　ビット列							
		上位4ビット				下位4ビット			
ECCデータブロック1	55h	0	1	0	1	0	1	0	1
ECCデータブロック2	75h	0	1	1	1	0	1	0	1
ECCデータブロック3	55h	0	1	0	1	0	1	0	1
ECCデータブロック4	4Dh	0	1	0	0	1	1	0	1
ECCデータブロック5	55h	0	1	0	1	0	1	0	1
ECCデータブロック8	97h	1	0	0	1	0	1	1	1
修正済セキュリティ情報	55h	0	1	0	1	0	1	0	1

【書類名】　　要約書

【要約】

【課題】　セキュリティ性を高めた光ディスク装置のセキュリティ管理方法を提供する。

【解決手段】　読み出し対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程Ｓ２２と、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程Ｓ２４とを含み、正当セキュリティ情報を読み出し対象となるデータの処理に供する光ディクス装置のセキュリティ管理方法によって上記課題を解決できる。

【選択図】　　図６

出　願　人　履　歴　情　報

識別番号　　〔０００００１８８９〕

１．変更年月日　　１９９３年１０月２０日
［変更理由］　住所変更
住　所　　大阪府守口市京阪本通２丁目５番５号
氏　名　　三洋電機株式会社